



Huishoudelijk reglement

Bijlage 1: Standaardvoorzorgmaatregelen ter preventie van infectieziekten in het Regionaal Ziekenhuis Heilig Hart Leuven

1 Strikte naleving van handhygiëne

Tijdens directe of indirecte patiëntenzorg, schoonmaak van de kamers en het bereiden en distribueren van voedsel is de stagiair(e) verplicht de handhygiënerichtlijnen strikt na te leven.

Het ontsmetten van de handen met handalcohol is verplicht:

- Voor patiëntencontact
- Na patiëntencontact
- Vóór een zuivere/invasieve handeling
- Na contact met lichaamsvochten en slijmvliesen
- Na contact met de directe patiëntenomgeving

Iedere stagiair(e) dient de handen te wassen

- Na gebruik van het toilet
- Na het snuiten van de neus
- Vóór en na het eten
- Vóór het manipuleren, bereiden en verdelen van voedingsmiddelen
- Als de handen zichtbaar bevuild zijn (nadien de handen supplementair desinfecteren met handalcohol)
- Na het verlaten van de kamer van een patiënt in isolatie (zie isolatiekaarten).

Het dragen van polshorloges, festivalbandjes, haarrekjes rond de pols, armbanden of ringen (incl. trouwring) is niet toegelaten zodra beroepskledij gedragen wordt!

Een piercing wordt als een juweel gezien. Indien een piercing een besmettingsbron is voor de patiënt of hinderlijk is bij de behandeling/verzorging van de patiënt dient deze te worden verwijderd. Een goede hygiëne van de piercing is belangrijk.

De vingernagels moeten goed verzorgd, proper, kortgeknipt en vrij van nagellak of kunstnagels zijn. Korte mouwen zijn ook een vereiste bij patiëntenzorg.

Lange haren dienen samengebonden te worden (het haar mag niet in contact komen met de kledij of de patiënt). Het haar is steeds verzorgd. Baard en snor moeten goed verzorgd en kortgeknipt zijn (baard mag niet in contact komen met de kledij of de patiënt).

2 Beleid persoonlijke beschermingsmiddelen

Indien er toch kans is op contact met bloed, lichaamsvochten, excreties (faeces en urine) en secreties (uitz. zweet), gebruikt men persoonlijke beschermingsmiddelen. Probeer bevuilding van kleding en huid te vermijden bij het verwijderen van persoonlijke beschermingsmiddelen. Verwijder deze steeds voor het verlaten van de kamer. Persoonlijke beschermingsmiddelen zijn op de afdeling aanwezig.

- Wegwerphandschoenen

Draag handschoenen bij potentieel contact met bloed of ander infectieus materiaal, slijmvliesen, niet-intacte huid of potentieel besmette intacte huid. Pas de keuze van de handschoenen aan de aard van het werk aan.

- Verwijder handschoenen onmiddellijk na contact met de patiënt en zijn omgeving.
- Draag nooit dezelfde handschoenen voor de verzorging van 2 patiënten
- Was/desinfecteer handschoenen niet
- Vervang handschoenen bij overgang van een besmette lichaamszone naar een zuivere lichaamszone
- Na het verwijderen van handschoenen, worden de handen gedesinfecteerd.

- Schorten

- Draag een (wegwerp) halterschort om de huid te beschermen en bevuilding en besmetting van de kleding te vermijden tijdens procedures en zorgactiviteiten waarbij contact met bloed, lichaamsvochten, secreties en excreties verwacht kan worden.
- Draag een (wegwerp) isolatieschort bij contact met een patiënt in isolatie met een besmettelijke aandoening. Zie hiervoor de respectievelijke isolatieprocedures.

- Mond-, neus- en oogbescherming

- Gebruik persoonlijke beschermingsmiddelen om de slijmvliesen van ogen, neus en mond te beschermen tijdens procedures en zorgactiviteiten waarvan vermoed kan worden dat ze spatten van bloed, lichaamsvochten, secreties of excreties veroorzaken.
- Tijdens procedures die een aerosol teweegbrengen, bvb bronchoscopie, aspiratie, draagt men een masker én een bril of een face shield.

- Muts

- Gebruik persoonlijke beschermingsmiddelen om de haren te beschermen (wegwerp muts) procedures en zorgactiviteiten waarvan vermoed kan worden dat ze spatten van bloed, lichaamsvochten, secreties of excreties veroorzaken die op haar terecht kan komen. Vaak zal dit op plaatsen zijn waar er veel potentieel bloedverlies is zoals bvb. een operatiekwartier.
- Mogelijks dient een muts gedragen te worden bij een patiënt in isolatie. Zie hiervoor de respectievelijke isolatieprocedures.

- Schoenen

- Draag steeds schoenen die afwasbaar zijn zodat mogelijke spatten van bloed, lichaamsvochten, secreties en excreties, onmiddellijk verwijderd kunnen worden.
- Op plaatsen met potentieel bloedverlies zoals bvb. een operatiekwartier, dient speciaal schoeisel voorzien te worden (klompen).

3 De stagiair(e) respecteert de principes van asepsie

Alles wat in aanraking geweest is met de patiënt is potentieel besmet en wordt:

- Indien single use: als afval verwijderd
- indien herbruikbaar: gereinigd en gedesinfecteerd na gebruik

Bij een patiënt mag enkel zuiver (nieuw of ontsmet) materiaal gebruikt worden.

Indien huid- of slijmvliesbarrière doorbroken wordt, moet het gebruikte materiaal steriel zijn.

Er wordt een strikte scheiding gehandhaafd tussen besmet en gereinigd materiaal, ontsmet of steriel materiaal.

4 De stagiair(e) dient een verzorgd voorkomen te hebben

Alle stagiairs ontvangen een uniform van het ziekenhuis tijdens hun stage.

Een uniform of schort met korte mouwen, zonder persoonlijke kledingstukken is een voorwaarde voor een goede hygiëne. Het uniform mag alleen gedragen worden op het domein van het ziekenhuis.

Het Regionaal Ziekenhuis Heilig Hart, Leuven kent verschillende kledijtypes:

- Lange doktersjas met oprolbare mouwen die over de persoonlijke kledij gedragen wordt.
Uitzondering : labo: lange mouwen toegelaten om onderarmen te beschermen tegen spatten van patiëntenmateriaal of chemicaliën. Het uniform wordt zelf voorzien door de stagiair(e) en bij voorkeur dagelijks verversd én bij zichtbare bevuiling. De kledij wordt op zo hoog mogelijke temperatuur (60-90°C) gewassen.
- Een werkuniform: jas met korte mouwen en broek die in de plaats van de persoonlijke kledij gedragen wordt. De stagiair ontvangt een uniform van het ziekenhuis om te dragen tijdens de stage. Dit uniform wordt dagelijks verversd én bij zichtbare bevuiling. De stagiair kleedt zich om in de toegewezen kleedkamers op het domein van het ziekenhuis.

Kledij bevuild met bloed of lichaamsvochten moeten zo snel mogelijk vervangen worden

Warme en koude periodes

- Tijdens koude periode is het toegestaan warme kledij te dragen onder de arbeidskledij. Persoonlijke kledij onder de arbeidskledij mag maximum tot ellebooghoogte komen.
Het is toegestaan om een warm, eigen vestje te dragen wanneer je buiten gaat. Tijdens de zorg en patiëntencontact is een vestje niet toegestaan.
- Tijdens warme periode kan de stagiair kiezen voor het dragen van een polo, aangeboden door het ziekenhuis. Deze polo heeft geen zakken. Het dragen van persoonlijke T-shirt is nooit toegestaan.

5 Hoofddoeken en mutsen

Hoofddoeken

- Het ziekenhuis beschikt over witte hoofddoeken (werkkledij) die aan stagiairs worden uitgeleend. Deze worden door het ziekenhuis gewassen en elke dag omgeruild.
In afwachting van het beschikken van een witte hoofddoek die door het ziekenhuis wordt aangeboden mag de medewerker en de student zijn eigen hoofddoek dragen indien onderstaande regels gevolgd worden.
- Voor stagiairs werkzaam op niet-kritische verpleegafdelingen, medisch technische diensten, logistieke diensten, administratieve diensten is het dragen van een hoofddoek toegelaten, mits het volgen van onderstaande regels
 - o De hoofddoek is wit van kleur
 - o De hoofddoek mag enkel het haar bedekken met een knoop achteraan (dus niet over de kleding dragen). Een hoofddoek tot onder de kin mag niet
 - o De hoofddoek mag tijdens de uitvoering van werkzaamheden niet in contact komen met (de omgeving van) de patiënt of met patiëntenmateriaal
 - o De hoofddoek wordt dagelijks vervangen door een propere hoofddoek en direct bij zichtbare bevuilding. De hoofddoek moet bestand zijn tegen wassen op een temperatuur van 60°C of hoger.
- Voor kritische afdelingen (Operatiekwartier, intensieve zorgen, neonatologie) is het dragen van hoofddoek niet toegelaten. Zorgverleners die een hoofddoek wensen te dragen dienen dit te vervangen door een wegwerpmuts)

Foto's

Wat Kan	Wat kan niet
	

Mutsen:

Een muts wordt gebruikt om haren volledig te bedekken en wordt dagelijks vervangen én bij het verlaten van de afdeling én bij accidentele bevuilding met lichaamsvochten

Stagiairs in de keuken en cafetaria moeten steeds een witte haarmuts dragen waarin alle haren gestoken worden.

Stagiairs op OK, CSA, URG en in de sectiozaal op verloskwartier moeten steeds een groene haarmuts dragen waarin alle haren gestoken worden.

6 Schoeisel

Schoenen moeten aan volgende minimumvoorwaarden voldoen :

- Hygiëne :
 - Schoenen moeten goed onderhoudbaar / van goed te reinigen materiaal zijn
 - Aan de voorkant (de teenzijde) gesloten omdat het niet ondenkbaar is dat scherp materiaal zoals scalpels, naalden,... tijdens de werkzaamheden op de grond kan vallen
- Preventie van vallen :
 - Loopzool met antislip eigenschappen
 - Steun aan de hiel (door riempje of volledig gesloten schoen)

Schoeisel bevuild met bloed en lichaamsvchten moet onmiddellijk gereinigd en ontsmet worden.

7 Hoest- en nieshygiëne

Tijdens het werk worden papieren zakdoekjes gebruikt. Na gebruik worden deze direct weggegooid en wordt handhygiëne toegepast.

Gebruikte zakdoekjes in de broekzak worden als een besmettingsbron beschouwd.

Algemene regels rond hoest- en nieshygiëne:

- Bedek neus en mond als je hoest of niest. Gebruik bij voorkeur een papieren zakdoek of hoest anders in de elleboogplooï.
- Hoest niet in de richting van iemand anders
- Gooi de papieren zakdoek onmiddellijk in de vuilbak
- Was na het niezen of hoesten uw handen met water en zeep of ontsmet ze met handalcohol

In het ziekenhuis is het aanbevolen om een mondneusmasker te dragen in de gangen van het ziekenhuis en bij direct patiëntencontact, wanneer je verkoudheidssymptomen ervaart.

8 Prikongevallen vermijden

De stagiair(e) stelt alles in werking om prikongevallen te vermijden. Ze vergewist zich van de in het Regionaal Ziekenhuis Heilig Hart Leuven geldende procedures betreffende het gebruik van scherpe voorwerpen en leeft deze ook na (zie procedure op Hartlink “veilig injecteren”).

De eerste EHBO maatregelen dienen tevens onmiddellijk worden toegepast.

9 Hepatitis B vaccinatie

Op de afdelingen waar er rechtstreeks contact mogelijk is met bloed, of waar personen verblijven die mogelijk besmet zijn met het hepatitis B virus is hepatitis B vaccinatie noodzakelijk.

De stagiair(e) die niet gevaccineerd is tegen hepatitis B neemt contact op met de arbeidsgeneeskundige dienst van de school.

10 Tuberculinetest

Een tuberculinetest is verplicht bij blootstelling aan het tuberculoserisico voor de eerste stage en verder jaarlijks tijdens de volgende stages.

11 Beroepsziekten

Elke ziekte of aandoening die mogelijks verband houdt met het werk dient onmiddellijk, gesignaleerd te worden aan de arbeidsgeneesheer.

12 Ongeval tijdens de stage

Arbeidsongevallen worden onmiddellijk gemeld aan de onderwijsinstelling. Een prikongeval met een gebruikte injectienaald is een arbeidsongeval. Na een prikongeval onmiddellijk contact opnemen met de arbeidsgeneesheer van de onderwijsinstelling.

13 Andere ziekten

Een stagiair(e) die drager is van een ziekte, die tijdens de normale werkactiviteiten kunnen overgedragen worden op andere personen, moeten onmiddellijk de arbeidsgeneesheer op de hoogte brengen.

14 Zwangerschappen

Zwangerschappen dienen onmiddellijk gemeld te worden aan de stageplaats.

Indien nodig zal de arbeidsgeneesheer oordelen of er preventiemaatregelen moeten getroffen worden ter bescherming van moeder en/of kind. (zie ook bijlage 2: risico-evaluatie moederschapsbescherming)

15 Eten en drinken

Eten en drinken is niet toegelaten waar patiëntengebonden werkzaamheden plaatsvinden of waar wordt gewerkt met patiëntenmateriaal (bvb. verpleegkar).

Er mogen geen warme maaltijden van de cafetaria naar de dienst worden gebracht. Indien het uitzonderlijk, bijvoorbeeld ten gevolge van tijdsgebrek, niet mogelijk is om naar de cafetaria te gaan, dan mag de stagiair(e) een koude maaltijd (sla, koude spaghetti,...) of broodmaaltijd op de dienst nuttigen, of mag een warme maaltijd met een deksel meegenomen worden.

Bijlage 2:artikel discretieplicht, informatieveiligheidsbeleid, GDPR

Stagiairs dienen zich aan te melden op de website [Stages Heilig Hart Leuven \(hhleuven.be\)](http://Stages.HeiligHartLeuven.be). Deze gegevens worden gebruikt voor de aanmaak van inloggegevens.

Bijlage 5 - arbeidsreglement

Informatieveiligheidsbeleid

Context

Het Regionaal Ziekenhuis H. Hart bezit en beheert persoonlijke gegevens van zijn patiënten en zijn medewerkers (dit is ruimer dan alleen personeelsleden). Zo is onder andere het medisch dossier van patiënten confidentieel en dient het als dusdanig behandeld te worden.

Door middel van het "Informatieveiligheidsbeleid" bevestigt de Directie van het ziekenhuis het belang van de beveiliging van informatie binnen het ziekenhuis. Deze dient verzekerd te worden van een strikte opvolging van richtlijnen door:

- Het personeel, medewerkers alsook derden (zelfstandigen, stagiairs, vrijwilligers, ...) van het ziekenhuis wat betreft de behandeling van informatie en IT systemen;
- Diensthoofden, leidinggevend en directie wat betreft monitoring van inbreuken tegen de richtlijnen;

Het informatieveiligheidsbeleid levert de richtlijnen die op te volgen zijn.

Definities

Het doel van informatieveiligheid is de informatie te beschermen tegen interne en externe bedreigingen, accidenteel of intentioneel. In deze context verzekert informatieveiligheid:

- De **confidentialiteit** van informatie en voorkomt deze het openbaar maken van deze informatie naar onbevoegden toe, zowel intern als extern. Het ziekenhuis bezit persoonlijke informatie van zijn patiënten, personeel, derden, ... en dient deze ter dege te beveiligen omwille van de wetgeving omtrent Data Privacy. Niet-naleving van deze wetgeving kan leiden tot juridische vervolging. Daarom dient alle informatie van onze patiënten, werknemers en derden in de ruime zin van het woord, als hoogst confidentieel beschouwd te worden. De Apps waarmee je patiëntgegevens kan opvragen mogen enkel gebruikt worden op hardware (smartphone, tablet,...) eigendom van het ziekenhuis:
 - de apps met betrekking tot KWS (Companion, bed reiniging, CPV,...)
 - apps voor opvolging van live data (monitoring patiënten)
 - apps voor
- De **integriteit** (correctheid) van informatie. Zo kan bijvoorbeeld het foutief veranderen van (medische) gegevens leiden tot een verkeerde behandeling, met zware (medische) gevolgen. Om deze reden is een correcte verwerking alsook het correct ter beschikking stellen van deze informatie samen met een goede beveiliging van informatie zeer belangrijk.
- De permanente **beschikbaarheid** van informatie en IT systemen, die belangrijker wordt naarmate onze (medische) activiteiten meer geïnformatiseerd worden. Zo kan bijvoorbeeld de onbeschikbaarheid van IT systemen leiden tot een laattijdige of verkeerde (medische) behandeling.

Informatieveiligheid betreft alle vormen van informatie, zowel in elektronische als hardcopy formaat. Voorbeelden van informatie zijn aldus:

- Informatie op de diverse computers: waaronder servers, PC's, Thin Client's, laptops (zowel deze van het ziekenhuis als deze van de artsen), diverse folders, e-mail systemen, het elektronisch patiënten dossier zowel het verpleegkundige, het medische alsook het medicatiedossier, ...
- Informatie op andere informatiedragers, zoals USB stick, CD ROM, ea. maar ook evengoed via de 'cloud' storage oplossingen van de diverse leveranciers.
- Papieren patiënten dossier, afgeprinte rapporten, resultaten en protocol's, röntgenfoto's, patiënt afspraakbevestigingsbrieven, verwijsbrieven, ...

Het ziekenhuis zal alle nodige maatregelen nemen teneinde de confidentialiteit, integriteit en beschikbaarheid van informatie en IT systemen te vrijwaren.

Richtlijnen voor het personeel

Vele medewerkers van het Regionaal Ziekenhuis H. Hart in welk statuut dan ook (zelfstandigen, werknemers, stagiairs, vrijwilligers, ...) hebben toegang tot medische en / of gegevens van patiënten en derden (personeel) en zijn als dusdanig mede verantwoordelijk voor het vrijwaren van de confidentialiteit van deze gegevens.

Als confidentiële informatie wordt onder andere beschouwd:

- Administratieve en medische gegevens van patiënten, onder elke hoedanigheid, zo bijvoorbeeld een dossier, verslagen, rapporten, scans, ...
- Administratieve gegevens van personen werkzaam in het ziekenhuis, inclusief dokters, tijdelijke werknemers, stagiairs, consultants, vrijwilligers,...
- Documenten die betrekking hebben op het beheer van het ziekenhuis.

Het is strikt verboden confidentiële gegevens te delen met onbevoegden, dit geldt zowel voor elektronische documenten, als voor documenten op papier. Ingeval van twijfel bij een aanvraag van een derde dient het diensthoofd, al dan niet bijgestaan door de Hoofdgeneesheer (medische) of een directielid (administratief), geconsulteerd te worden.

Alle medewerkers dienen de nodige maatregelen te nemen om confidentiële informatie te beveiligen. De richtlijnen hiervoor worden hieronder gegeven, ze gelden voor alle medewerkers tewerk gesteld in het ziekenhuis, inclusief dokters, tijdelijke werknemers, stagiairs, consultants, vrijwilligers, ...

Toegang tot de IT systemen met user accounts en paswoorden

De meeste confidentiële informatie bevindt zich in elektronisch formaat op de diverse informatie systemen van het ziekenhuis, de medewerkers hebben een persoonlijk gebruikersprofiel om de nodige systemen te gebruiken.

Gebruikersprofielen en paswoorden zijn te allen tijde toewijsbaar aan één individu, ze zijn dus persoonlijk en mogen onder geen enkele omstandigheid gedeeld worden met anderen, ook niet met directe collega's, enige andere medewerker of met familieleden.

Indien u uw paswoord toch met anderen deelt, dan kan het mogelijk misbruik steeds worden teruggebracht tot uw persoon. U zal te allen tijde aansprakelijk blijven voor dit misbruik welke in uw naam is gebeurd. Ingeval u vermoedt dat uw paswoord gekend is door anderen, dan moet u dit paswoord zo snel mogelijk wijzigen.

Alle acties op de IT systemen kunnen worden geregistreerd in logs, die kunnen worden nagekeken, conform de bepalingen in het arbeidsreglement, wanneer er zich een vermoeden van onregelmatigheden heeft voorgedaan.

Toegang tot de IT systemen is beveiligd door paswoorden, waarvoor de volgende adviserende regels gelden:

- Minimum lengte 6 letters of cijfers, waarbij een lengte van 14 karakters wordt geadviseerd met minstens 2 cijfers, hoofdletters en tekens;
- Elke 90 dagen proactief te wijzigen, waarbij geen voorgaande wachtwoorden mogen herhaald worden

Teneinde misbruik te voorkomen, is het belangrijk dat u bij voorkeur afmeld wanneer u het werkstation verlaat (voor een langere periode) en dat u uw werkstation (PC, laptop of Thin Client) op zijn minst blokkeert wanneer u (voor een kortere periode) uw werkplek verlaat. Het blokkeren van het werkstation gebeurt door tegelijk CTRL-ALT-DELETE in te drukken.

Ingeval u merkt of er een vermoeden is dat het werkstation van een medewerker door een derde misbruikt werd, dient u zo snel mogelijk uw diensthoofd, leidinggevende of directiehoofd te informeren.

Professioneel gebruik van de IT systemen

De IT systemen van het ziekenhuis mogen enkel gebruikt worden voor professionele doeleinden, niet-professioneel gebruik of gebruik voor persoonlijke doeleinden is niet toegestaan. (zie artikels 41-42 van het arbeidsreglement).

Dit omvat onder andere het gebruik van internet en e-mail. Alle acties op de IT systemen kunnen in logs worden geregistreerd en kunnen als dusdanig geconsulteerd worden ingeval van onregelmatigheden of een vermoeden hiervan.

De IT systemen (PC's, laptops, enz...) worden u ter beschikking gesteld door enerzijds het ziekenhuis en anderzijds door de betrokken artsen, het is uw verantwoordelijkheid deze op een verantwoorde wijze te gebruiken en als een goede huisvader te hanteren.

Dit omvat ook draagbare toestellen of andere devices die al dan niet aan individuele werknemers toegewezen zijn.

Het spreekt voor zich dat elke manipulatie van deze toestellen risico's inhouden, waarbij men steeds dient toe te zien op de risico's. Zo is het bijvoorbeeld niet raadzaam om deze onbeheerd achter te laten in de wagen (ook niet in de koffer) of op publieke plaatsen, bij reizen moeten ze als handbagage meegenomen worden,

Enkel toegelaten software, apps worden geïnstalleerd en gebruikt op PC's, laptops, smartphones eigendom van het ziekenhuis. Niet toegelaten software, apps kan de integriteit of continuïteit van deze systemen schaden en problemen creëren wat betreft software, apps licenties. Daarom is het verboden niet-toegelaten software, apps, tools, enz...op uw PC of laptop te installeren. Het is ook verboden de configuratie van uw PC of laptop te wijzigen.

Belangrijke of confidentiële documenten mogen niet in publieke folders bewaard worden, deze zijn toegankelijk voor allen en worden op regelmatige basis gescreend. Wanneer documenten dienen gedeeld te worden binnen het departement, kan er een departementale folder ter beschikking gesteld worden en is deze de geschikte plaats om het document te bewaren. Andere confidentiële documenten dienen in uw persoonlijke folder bewaard te worden. Ingeval van twijfel: consulteer uw diensthoofd/leidinggevende of IT-helpdesk. Er mogen daarenboven geen data, foto's, video's of muziek bestanden van persoonlijke titel opgeslagen worden op de dataservers van het ziekenhuis, noch op de lokale werkstations.

Fysische beveiliging

Informatieveiligheid omvat ook de fysische beveiliging van papieren documenten, PC's, laptops, medische apparatuur, medicatie,... Deze moeten op een veilige plaats bewaard worden, die niet toegankelijk is voor onbevoegde personen.

Daarom is het belangrijk:

- Deuren van bureaus en plaatsen te sluiten (met sleutel of badge wanneer aanwezig), wanneer men deze voor een langere tijd (vb lunchpauze, koffiebreek) verlaat;
- Kasten met confidentiële informatie, medicatie, ... met sleutel of code op slot te doen buiten de werkuren;
- Geen confidentiële documenten te laten rondslingeren, maar in kasten of bureaus te steken en deze op slot te doen;
- Door de elektronische archivering van de medische dossiers is het niet meer nodig deze op papier te bewaren. We beperken het afprinten van dossiers en documenten tot het noodzakelijke;
- Documenten te (laten) vernietigen, die niet langer nodig zijn. Indien de informatie confidentieel is, dienen hiervoor de versnipperaars gebruikt te worden.

Indien u verdachte of onbekende personen opmerkt op plaatsen waar deze niet hoeven te zijn, dient u deze vriendelijk aan te spreken met de vraag wat de reden van hun aanwezigheid is, en uw diensthoofd/leidinggevende of de preventieadviseur te contacteren wanneer nodig.

Aanvraag voor toegang tot confidentiële informatie

Wij ontvangen soms aanvragen tot het doorgeven van informatie. Een voorbeeld is een huisarts die medische informatie vraagt in verband met de behandeling van een patiënt.

Voor zulke aanvragen dient geverifieerd te worden of:

- De aanvrager de persoon is die hij zegt te zijn;
- De aanvraag gerechtvaardigd is. Hierbij dient bijvoorbeeld gecheckt te worden in het elektronisch dossier of er 'informed consent' werd ondertekend door de patiënt, of de aanvrager inderdaad de informatie nodig heeft vanuit zijn functie, of de persoon inderdaad patiënt is bij de huisarts, enz...

Richtlijnen voor de diensthoofden/leidinggevenden

Daar waar het aan de medewerkers is de hiervoor vermelde richtlijnen te volgen, is het aan de diensthoofden en directie om na te gaan of de richtlijnen opgevolgd worden. Ingeval van inbreuken is het ook aan hen om correctieve of penaliserende acties te nemen, conform de bepalingen vermeld in het arbeidsreglement.

De hiervoor gedefinieerde richtlijnen zijn generiek en van toepassing op het hele ziekenhuis. Binnen de verschillende diensten kunnen nog specifieke richtlijnen gegeven worden, vanwege de specificiteit van de afdeling.

Daarom is het aan de afdelingshoofden/ leidinggevenden te bepalen of er specifieke noden zijn wat betreft informatieveiligheid en hiervoor richtlijnen te geven of maatregelen te nemen. Voorbeelden hiervan kunnen zijn:

- Afsluiten met sleutel van een bepaalde kast met gevaarlijk producten;

- Plaatsen van een versnipperaar voor confidentiële documenten;
- Aanvraag voor een extra badgereader of camera om toegang te bewaken tot een kamer met dure medische apparatuur.
- Aanvraag tot beveiliging van een netwerkfolder waarin zich confidentiële documenten bevinden. Of het verplaatsen van deze documenten naar een persoonlijke folder.

Daarnaast is het ook aan de diensthoofden/leidinggevenden om te bepalen tot welke systemen en toepassingen de personeelsleden van hun afdeling toegang dienen te krijgen. Aanvragen voor toegang van personeelsleden zullen in de toekomst via het document "items in –en uitdienst" gedaan worden, het is aan de diensthoofden/leidinggevenden deze aanvragen juist uit te voeren.

Algemene richtlijn hierbij is dat een medewerker slechts toegang dient te krijgen tot systemen en toepassingen, die hij of zij nodig heeft voor het uitvoeren van zijn taken, en niet meer.

Het is aan elk diensthoofd/leidinggevende:

- De opvolging van bovenstaande richtlijnen in zijn afdeling na te gaan en bij te sturen waar nodig;
- De nodige maatregelen vast te leggen wat betreft beveiliging van confidentiële informatie, bureaus, kasten, PC's, laptops,... in zijn afdeling.
- Er zullen regelmatig audit trails worden uitgevoerd op instructie van de directie, zoals omschreven in Art 40 hierboven.

Bijlage 7 – arbeidsreglement

Begripsomschrijving 'discretieplicht'

De discretieplicht omvat het geheel van deontologische, ethische,... regels die dienen gerespecteerd te worden binnen het Regionaal Ziekenhuis H. Hart, in het omgaan met medische en niet-medische gegevens over patiënten, collega's, bezoekers, enz.

Het respect voor de discretieplicht is ruimer dan alleen het respect voor het medisch beroepsgeheim of de privacywetgeving. Voor de inhoud van het medisch beroepsgeheim stricto sensu verwijzen wij naar de specifieke reglementeringen ter zake (o.a. art. 458 Strafwetboek). *

Het respect voor de discretieplicht is een algemeen en absoluut principe

Een strikt respect voor de discretieplicht is een fundamenteel principe voor "alle" personeelsleden, geneesheer-specialisten, vrijwilligers, stagiaires,.. van het Regionaal Ziekenhuis H. Hart. Het betreft hier niet alleen de personeelsleden die rechtstreeks met de zorg verbonden zijn, doch ook dezen die niet rechtstreeks met de zorg verbonden zijn en al diegenen die zich in het kader van hun beroepsuitoefening of hun opleiding binnen het Regionaal Ziekenhuis H. Hart bewegen.

Een groot aantal personeelsleden kreeg tijdens hun beroepsopleiding reeds een meer uitvoerige toelichting met betrekking tot de toepassing van de discretieplicht binnen een ziekenhuisomgeving. Voor sommigen is dit niet het geval geweest, of is dit reeds lang geleden. Bovendien zijn de risico's om de discretieplicht te overtreden, geëvolueerd onder meer door het inschakelen van informaticatoepassingen in het zorggebeuren.

Het Regionaal Ziekenhuis H. Hart vindt het dan ook uiterst belangrijk om de draagkracht van de discretieplicht in het dagelijks werk continu onder de aandacht te houden.

Wat houdt het respect voor de discretieplicht binnen het Regionaal Ziekenhuis H. Hart in?

De discretieplicht respecteren betekent dat u de informatie die u krachtens uw beroep weet, geheimhoudt.

De discretieplicht heeft in het algemeen betrekking op alles wat u ziet, hoort, verneemt, vaststelt, ontdekt of opvangt in het kader van de uitoefening van uw beroep. Het gaat hierbij niet alleen om gegevens van medische aard, doch tevens over alle andere inlichtingen van vertrouwelijke aard.

De discretieplicht respecteren is niet eenvoudig: De 'regels' zijn immers niet sluitend bepaald.

Daarenboven is men niet steeds voorbereid op hoe te reageren op vragen van anderen. Of vraagt men zich bij zijn dagdagelijkse gedragingen niet altijd meer af of iets wel mag. Of denkt men dat men informatie mag doorgeven omdat de ontvanger ook door de discretieplicht gebonden is. Of is men te vlug overtuigd dat de praktische werkbaarheid toch wel dient te primeren.

Huidige bepalingen beogen dan ook een leidraad te zijn bij het omgaan met informatie over patiënten en over andere medewerkers uit respect voor de privacy waarop zij recht hebben. Iedere patiënt, ieder personeelslid en geneesheer-specialist, vrijwilliger, stagiair moet er immers op kunnen rekenen dat gegevens die verband houden met zijn aanwezigheid of beroepsuitoefening in het ziekenhuis als vertrouwelijk worden beschouwd.

Reglementaire bepalingen

Het respect voor de discretieplicht is opgenomen in diverse reglementen die van kracht zijn binnen het Regionaal Ziekenhuis H. Hart.

-Zo stelt het Medisch reglement tussen het Regionaal Ziekenhuis H. hart en de geneesheer-specialisten:

"De ziekenhuisartsen respecteren het recht op privacy van de patiënt en de vertrouwelijkheid van zijn of haar informatie, door toegang tot de gezondheidsinformatie te beperken en deze veilig te bewaren. "

-Voor de personeelsleden vermeldt het arbeidsreglement, artikel 39 beroepsgeheim:

"Het personeel zal de geheimhouding en de grootste discretie met de zieken, de familie en de bezoekers in acht nemen. Zij mogen volstrekt niets bekend maken van wat zij vernemen over de zieken, de behandeling of de identiteit van de patiënten, ook niet na het beëindigen van de arbeidsovereenkomst. Elkeen zal door zijn specifieke beroepsbezigheid steeds het beroepsgeheim eerbiedigen. Het Strafwetboek verbindt aan het misdrijf van schending van beroepsgeheim bovendien straffen.

Analoge bepalingen inzake de discretieplicht werden opgenomen in het vrijwilligerscontract alsmede in de stageovereenkomst.

Daarnaast gelden ook de bepalingen van het Reglement inzake de toegang tot het Klinisch Werkstation/Nexus Health, het eventuele huishoudelijk reglement van een dienst, de procedure met betrekking tot inzage en afschrift van het medisch dossier, enz., waarin voor specifieke doelgroepen meer specifieke of bijkomende bepalingen inzake de discretieplicht opgenomen zijn.

In aanvulling bij deze bestaande reglementaire bepalingen heeft huidige gedragscode tot doel het belang van het respect voor de discretieplicht binnen het Regionaal Ziekenhuis H. Hart nogmaals te benadrukken en de globale bepalingen m.b.t. de discretieplicht concreter in te vullen.

Enkele concrete situaties

Hieronder enkele concrete regels m.b.t. het respecteren van de discretieplicht in een aantal herkenbare situaties:

U kan enkel inzage nemen van een patiëntendossier of gegevens uit het patiëntendossier onder welke vorm ook, mits toestemming van de verantwoordelijke geneesheer-specialist en in zoverre dit nodig is voor de zorgverlening. De toestemming van de verantwoordelijke geneesheer-specialist kan ook globaal (d.w.z. niet geïndividualiseerd per patiënt) of impliciet zijn (af te leiden uit de opdracht), tenzij hierover andersluidende afspraken werden gemaakt.

U bent niet gerechtigd om louter op eigen initiatief gegevens in uw persoonlijk medisch dossier of personeelsdossier te raadplegen. De Wet op de patiënten rechten en de privacywetgeving kennen u welbepaalde rechten toe (recht op het vragen van inzage en eventueel afschrift, recht op mededeling), doch kent u geen onmiddellijk rechtstreeks inzagerecht toe.

De geneesheer-specialist die met betrekking tot zichzelf of zijn familieleden optreedt als (mede)behandelende arts en als dusdanig bekend gemaakt werd, heeft uiteraard wel een rechtstreeks inzagerecht in de betreffende medische gegevens.

Medische secretariaten en archiefruimten zijn in principe niet toegankelijk voor personen die bij de concrete dienstverlening van die diensten niet betrokken zijn.

Met uitzondering van de informatie die u beroepshalve moet verstrekken en tenzij de patiënt duidelijk door één of andere reactie of na bevraging te kennen heeft gegeven dat men van deze zwijgplicht is ontslagen: (met betrekking tot het medisch beroepsgeheim geldt dat de patiënt de geneesheer-specialist in een aantal gevallen op eigen aangeven van zijn zwijgplicht kan ontheffen, doch hij/zij is niet verplicht om daar op in te gaan.) mag u geen enkele mededeling doen omtrent namen van patiënten die u heeft behandeld of van wie u weet dat ze in het ziekenhuis

zijn, zullen komen, of geweest zijn, noch betreffende de dienst waar of de aandoening waarvoor zij verzorgd worden.

Dit geldt zowel intern als extern, en dit zowel ten aanzien van collega's als ten aanzien van andere patiënten, familie, vrienden, enz.

Bovendien geldt dit principe ook bij een politie- of een gerechtelijk onderzoek. Er bestaan hieromtrent welomschreven procedures.

Indien medische informatie binnen een multidisciplinaire groep moet gedeeld worden om een goede behandeling mogelijk te maken, moet dit op een correcte manier gebeuren, met eerbied voor de privacy en de waardigheid van de patiënt en waarbij overbodige details achterwege worden gelaten.

Tot slot wordt opgemerkt dat deze bepalingen uiteraard evenzeer gelden ten aanzien van personeelsleden die niet rechtstreeks in de zorgverlening ingeschakeld zijn, doch die tijdens of in het kader van de uitoefening van hun functie bij het Regionaal Ziekenhuis H. Hart medische informatie vernemen (bv. personeelsleden Medische Administratie, Inschrijvingen,...).

U mag inlichtingen per telefoon slechts verstrekken indien u zeker is van de identiteit van uw gesprekspartner, deze persoon inderdaad recht heeft op die informatie (bv. ouders) of bij de behandeling of de nazorg betrokken is (bv. huisarts), én op voorwaarde dat de verantwoordelijke geneesheer-specialist hiermee akkoord gaat.

Het enkel uit nieuwsgierigheid of sensatiezucht bespreken van vertrouwelijke (medische) informatie over bekende personen, politieke personaliteiten, artiesten, sportlui, artsen, medestudenten, personen werkzaam in het ziekenhuis, enz. is een grove inbreuk op de discretieplicht.

Dit alles blijft van toepassing wanneer deze persoon overleden is.

Indien u iemand ontmoet die u kent, kan u uiteraard deze persoon begroeten, doch zonder verder in gesprek te gaan over zijn/haar aanwezigheid in het Regionaal Ziekenhuis H. Hart, tenzij deze persoon zelf hiertoe het initiatief neemt.

U dient er steeds over te waken dat u met collega's geen gegevens aangaande patiënten bespreekt of met de patiënt zelf geen vertrouwelijke gegevens over zijn toestand uitwisselt of opvraagt in ruimten waar u het risico loopt dat anderen kunnen meeluisteren (bv. cafetaria, kleedkamer, gang, wachtzaal, liften, bushalte). Indien dit door omstandigheden niet uitgesloten kan worden (bv. niet-verplaatsbare patiënten in gemeenschappelijke patiëntenkamer), dient u er voor te zorgen dat u de privacy van de patiënt maximaal respecteert (bv. met gedempte stem spreken, enz.).

Bij (wetenschappelijke) voordrachten moet de anonimiteit van patiënten zo zorgvuldig mogelijk bewaard worden (geen naam, geboortedatum, woonplaats, beroep, foto, namen op radiografische opnames, ...).

Het bekendmaken of publiceren van gegevens over patiënten of van situaties die zich tijdens het werk hebben voorgedaan via elektronische media (internetsites, discussiefora, sociale netwerken zoals Facebook en Twitter) is verboden.

Let er steeds op dat u geen documenten waarmee anderen gegevens van patiënten kunnen achterhalen achteloos laat rondslingeren (bv. kladblaadjes op nachtkastjes of in kleedkamers).

Klinische ervaringen kunnen, buiten het kader van de behandeling, enkel met collega's uitgewisseld worden op voorwaarde dat de besproken patiënt op geen enkele wijze herkenbaar is en het gesprek niet plaatsvindt in een openbare ruimte.

Medische dossiers kunnen in het kader van een wetenschappelijke studie worden geraadpleegd voor zover dit onderzoek geschiedt onder toezicht van een geneesheer-specialist en mits schriftelijk akkoord van een vast staf lid van de dienst waartoe het dossier behoort, indien het medisch geheim niet wordt geschonden en de procedure conform is met de wetgeving betreffende de rechten van de patiënt.

Inlichtingen over personeelsgegevens (bv. adres- of loongegevens) of andere gegevens (bv. dienstorganisatie, individuele uurroosters) mag u enkel meedelen conform de bepalingen van de wetgeving op de privacy.

Niet-publieke informatie over het Regionaal Ziekenhuis H. Hart (gegevens over de financiële situatie, statistische gegevens, enz.) waarvan u kennis krijgt tijdens of in het kader van de uitoefening van uw

functie, kan u enkel meedelen aan diegenen waaraan u dit gerechtigd bent te doen en in zoverre u deze informatie beroepshalve moet verstrekken.

In geval van twijfel doet u er best aan om de situatie met uw leidinggevende af te stemmen.

Specifiek aandachtspunt: het gebruik van computersystemen

Heel wat gegevens waarop de discretieplicht van toepassing is, werden geïntegreerd in geïnformatiseerde bestanden (bv. Klinisch Werkstation (afgekort: KWS), Saga, Sprint,...).

De toegang tot deze systemen is geregeld via een systeem van toegangscontrole, wat het Regionaal Ziekenhuis H. Hart toelaat om de toegang te beperken tot de geneesheer-specialisten, personeelsleden,... die deze informatie voor beroepsdoeleinden nodig hebben. Waar mogelijk en werkbaar, werden ook technische toegangsbeperkingen en -controles ingelast.

U maakt misbruik van de computersystemen door:

- gegevens op te vragen die u niet nodig heeft
- programmacodes te achterhalen en te gebruiken die niet voor u zijn vrijgegeven-de u gekende codes/paswoorden door te geven (Paswoorden van login-namen mogen nooit doorgegeven worden. Paswoorden van gemeenschappelijke login-namen mogen enkel aan bevoegden worden meegedeeld.)
- computerlijsten, etiketten of afdrukken met patiënten- of personeelsgegevens te laten rondslingeren of buitenshuis te verspreiden (bv. als klad- of tekenpapier)

Het Reglement inzake de toegang tot het Klinisch Werkstation regelt de toegang tot en het gebruik van het KWS. Enkele belangrijke aandachtspunten hierbij zijn:

- Van eenieder wordt verwacht dat hij uitsluitend informatie opzoekt om professionele redenen. Het opzoeken van andere informatie (bv. eigen medische gegevens of deze van familieleden wanneer men niet optreedt als (mede-)behandelende geneesheer-specialist, administratieve gegevens zoals data van afspraken of consultaties, kamernummer in functie van een privébezoek), het gebruik van de login of het codewoord van een andere persoon of het inkijken van een "openstaand patiëntencontact" wordt als een ernstige schending van de privacy en de discretieplicht beschouwd.
- De toegang tot KWS is geregeld via afgebakende gebruikerstoegangen. Om redenen van praktische en vlotte werkbaarheid is het technisch steeds mogelijk om een toegangsbeperking te doorbreken ("overrule"). Het respect voor de discretieplicht geldt echter ten allen tijde: een toegangsbeperking mag dan ook enkel om welbepaalde gerechtvaardigde redenen doorbroken worden.
- Indien u over een login en codewoord beschikt dat u toegang verleent tot het KWS, dient u dit geheim te houden. Indien u wenst dat één van uw medewerkers ook rechtstreeks toegang heeft tot bepaalde gegevens van het KWS waartoe u zelf gerechtigd bent, bent u niet geoorloofd om uw login en codewoord door te geven. Iedereen is immers persoonlijk verantwoordelijk voor de acties die onder zijn login in het KWS worden uitgevoerd. Indien nodig kan een gemotiveerde aanvraag gericht worden t.a.v. van de KWS-implementatieploeg teneinde een aparte login met afgebakende toegangsmogelijkheden voor uw medewerker te voorzien.
- Wanneer u in KWS werkt, dient u de "openstaande dossiers" tot een minimum te beperken en zeker nooit onbewaakt te laten. Gebruik dan ook "Beveilig scherm" (CTRL-B) uit het menu "Algemeen" om het KWS af te sluiten voor onbevoegde blikken wanneer u uw computer verlaat.
- Los van de "overrule" gebeurt voor elke patiënt een full audit. Dit betekent dat elke toegang tot het elektronisch dossier van elke patiënt gelogd wordt, wat een controle van alle acties in hun dossier mogelijk maakt.
- Iedereen die vermoedt dat onbevoegden zich via het KWS toegang verschaffen tot zijn elektronisch dossier of dat van anderen, kan dit via de behandelende geneesheer-specialist laten nagaan. Deze laatste zal, indien nodig, instaan dat de gepaste maatregelen getroffen worden.

Inbreuken op de discretieplicht worden gesanctioneerd

Diverse interne (bv. Medisch reglement, Arbeidsreglement, Reglement vrijwilligers,...) en externe (bv. strafwetboek) reglementen voorzien maatregelen die kunnen toegepast worden bij ernstige inbreuken op de discretieplicht.

Het Regionaal Ziekenhuis H. Hart zal bovendien niet nalaten de nodige stappen te ondernemen bij inbreuken op de discretieplicht door personen die zich in het kader van hun beroepsuitoefening of hun opleiding binnen het ziekenhuis bewegen, maar geen overeenkomst met het ziekenhuis hebben afgesloten.

* Artikel 458 van het Strafwetboek luidt als volgt: Geneesheren, heelkundigen, officieren van gezondheid, apothekers, vroedvrouwen en alle andere personen die uit hoofde van hun staat of beroep kennis dragen van geheimen die hun zijn toevertrouwd, en deze bekendmaken buiten het geval dat zij geroepen worden om in rechte of voor een parlementaire onderzoekscommissie getuigenis af te leggen en buiten het geval dat de wet hen verplicht die geheimen bekend te maken, worden gestraft met gevangenisstraf van acht dagen tot zes maanden en met geldboete van honderd euro tot vijfhonderd euro.

Bijlage 9 arbeidsreglement

Informatieplicht in uitvoering van de Europese verordening omtrent gegevensbescherming (zie ook de beleidsverklaring inzake gegevensbescherming en verwerking van persoonsgegevens van werknemers)

De persoonsgegevens van personeel worden verwerkt onder de verantwoordelijkheid van het Regionaal Ziekenhuis H. Hart vzw, Naamsestraat 105 te 3000 Leuven.

De gegevens worden uitsluitend verwerkt met het oog op de tewerkstelling van de betrokkenen in onze organisatie en de daaruit voortvloeiende administratieve en sociale verplichtingen. Deze verwerking is een noodzakelijke voorwaarde voor de uitoefening van de arbeidsovereenkomst die de betrokkene met onze instelling is aangegaan.

De betrokkene is contractueel verplicht om de gegevens te verstrekken die noodzakelijk zijn voor de administratieve en sociale verplichtingen die voortvloeien uit de arbeidsovereenkomst. Niet-noodzakelijke gegevens die vrijwillig door de werknemer in kwestie worden verstrekt, worden verwerkt op basis van het toestemmingscriterium. De betrokkenen heeft het recht zich te verzetten tegen de verwerking van vrijwillig verstrekte informatie. Hij heeft eveneens het recht om de verstrekte toestemming weer in te trekken. Dit doet evenwel geen afbreuk aan de rechtmatigheid van verwerkingen voorafgaand aan het intrekken van de toestemming.

De gegevens worden vertrouwelijk behandeld en enkel doorgegeven aan de bevoegde overheidsinstellingen, verzekeringsinstellingen, het sociaal secretariaat SD Worx, Tobania – HCPS, externe geneeskundige dienst, HR technologies die de gegevens eveneens vertrouwelijk behandelen.

Persoonsgegevens van werknemers worden bijgehouden zolang hun arbeidsovereenkomst met onze organisatie duurt. Sociale documenten dienaangaande worden, conform de toepasselijke wetgeving, tot 5 jaar na het einde van de arbeidsovereenkomst bijgehouden. Eventuele gezondheidsdossiers worden daarenboven, eveneens conform de toepasselijke wetgeving, 15 jaar na het ten einde nemen van de arbeidsovereenkomst bijgehouden. Na afloop van deze periodes worden de gegevens vernietigd.

De betrokkene heeft het recht om inzage te krijgen in zijn persoonsgegevens, alsook op de rectificatie van de opgeslagen gegevens. Hij beschikt eveneens over het recht om de verwijdering van zijn persoonsgegevens te vragen, voor zover de instelling niet wettelijk verplicht is om die gegevens te bewaren. De betrokkenen beschikt daarenboven over het recht op gegevensoverdracht.

Indien de betrokkenen van oordeel zou zijn dat de regelgeving rond de verwerking van zijn persoonsgegevens niet gerespecteerd wordt door de instelling, dan heeft hij het recht om een (gemotiveerde) klacht in te dienen bij de Privacy commissie.

Bijlage 3: Gedragscode Regionaal Ziekenhuis Heilig Hart Leuven

1. Voorwoord

Als zorginstelling dragen wij een bijzondere verantwoordelijkheid. Patiënten vertrouwen ons hun gezondheid toe, medewerkers rekenen op een veilige en respectvolle werkplek en de samenleving verwacht integriteit en professionaliteit en maatschappelijke verantwoordelijkheid.

Deze gedragscode concretiseert hoe wij onze missie, waarden en wettelijke verplichtingen dagelijks in praktijk brengen. Ze is geen louter formeel document, maar een leidraad voor professioneel gedrag en ethisch handelen in alle situaties.

Wij rekenen op ieders engagement om deze gedragscode actief na te leven en elkaar hierop aan te spreken.

2. Doel en toepassingsgebied

Deze gedragscode beschrijft de gedragsnormen die gelden binnen Regionaal Ziekenhuis Heilig Hart Leuven.

Ze is van toepassing op:

- alle medewerkers, ongeacht statuut
- artsen
- vrijwilligers
- stagiairs
- externe medewerkers en consultants

De gedragscode geldt voor gedrag:

- op de werkvloer
- in contacten met patiënten en bezoekers
- in samenwerking met externe partners
- in digitale communicatie en sociale media
- buiten de werkcontext wanneer dit impact heeft op het ziekenhuis of zijn reputatie

Deze code vormt een aanvulling op het arbeidsreglement, het informatieveiligheidsbeleid, het communicatiekompas en de toepasselijke wetgeving.

Voor de leesbaarheid wordt in deze gedragscode de term “medewerkers” gebruikt. Hiermee worden alle hierboven vermelde doelgroepen bedoeld.

3. Onze missie, visie en kernwaarden

Onze missie is zorg bieden die dichtbij en beter is.

Onze kernwaarden vormen het fundament van ons handelen:

Aandacht geven

Wij tonen oprechte betrokkenheid, luisteren actief en benaderen iedereen met respect en empathie.

Zorg bieden

Wij handelen betrouwbaar, zorgvuldig en professioneel, en leveren kwaliteitsvolle zorg.

Uitblinken

Wij streven naar continue verbetering, deskundigheid en innovatie.

Samenwerken

Wij werken interdisciplinair samen en communiceren open, respectvol en verbindend.

Deze waarden zijn richtinggevend voor alle gedragingen en beslissingen.

4. Onze ethische principes

Ons handelen wordt gestuurd door volgende principes:

- respect voor menselijke waardigheid
- rechtvaardigheid en gelijke behandeling
- professionele onafhankelijkheid
- vertrouwelijkheid en discretie
- verantwoordelijkheid en transparantie

Het ziekenhuis beschikt over een Commissie Medische Ethiek. Medewerkers en artsen kunnen ethische vragen vertrouwelijk voorleggen ter ondersteuning van zorgvuldige besluitvorming.

5. Professioneel gedrag

Wij gaan respectvol, professioneel en verbindend met elkaar om. Ons gedrag weerspiegelt onze waarden en draagt bij aan een veilige en positieve werkomgeving waarin samenwerking centraal staat.

We spreken elkaar respectvol aan bij gedrag dat we als niet professioneel ervaren. We staan open voor feedback.

We leveren goede zorg en volgen daarbij de interne procedures. Indien er geen procedures bestaan, werken we volgens evidence based principes.

5.1 Respect en waardigheid

Wij behandelen patiënten, bezoekers en collega's met respect, ongeacht achtergrond, overtuiging of functie.

Niet toegestaan:

- discriminatie
- pesterijen of intimidatie
- seksueel grensoverschrijdend gedrag
- agressie (verbaal of fysiek)

Respectvolle communicatie is de norm, zowel mondeling, schriftelijk als digitaal.

Wij spreken elkaar op een constructieve manier aan en staan open voor feedback. Wij dragen bij aan een werkomgeving waarin iedereen zich veilig en gerespecteerd voelt.

5.2 Samenwerking en collegialiteit

Kwaliteitsvolle zorg is teamwork.

Wij:

- communiceren open, correct en tijdig
- spreken elkaar respectvol aan
- nemen gezamenlijke verantwoordelijkheid
- delen informatie op een professionele en correcte manier

Wij gaan op een respectvolle manier om met meningsverschillen en zoeken samen naar oplossingen.

Leidinggevenden nemen hierin een voorbeeldrol op.

5.3 Diversiteit en inclusie

Wij waarderen diversiteit en creëren een inclusieve werkomgeving waarin iedereen zich welkom en gerespecteerd voelt.

Elke vorm van discriminatie of uitsluiting op basis van beschermde kenmerken is onaanvaardbaar.

6. Patiëntgerichte zorg en professionele grenzen

De patiënt staat centraal.

Wij:

- respecteren de autonomie en waardigheid van de patiënt
- handelen volgens het principe van informed consent
- bewaken professionele grenzen in de zorgrelatie

Het is verboden:

- misbruik te maken van een afhankelijkheidsrelatie
- persoonlijke of intieme relaties aan te gaan met patiënten
- persoonlijke contacten te onderhouden die de zorgrelatie beïnvloeden

7. Vertrouwelijkheid en gegevensbescherming

7.1 Algemeen principe

Alle medewerkers zijn gebonden aan een strikte discretieplicht.

Dit betekent dat alle informatie die men ziet, hoort of verneemt:

- vertrouwelijk wordt behandeld
- enkel gedeeld wordt indien noodzakelijk voor de functie
- nooit met onbevoegden wordt gedeeld

Deze verplichting blijft gelden na het beëindigen van de samenwerking.

7.2 Omgang met informatie

- Toegang tot patiëntgegevens gebeurt enkel indien nodig voor de functie
- Het inkijken van dossiers uit nieuwsgierigheid is verboden
- Gesprekken over patiënten gebeuren niet in openbare ruimtes
- Vertrouwelijke documenten, patiëntgegevens en andere gevoelige informatie worden bij afwezigheid of na afloop van de werkdag veilig opgeborgen en niet onbeheerd achtergelaten op werkplekken of in vergaderruimtes (clean desk-principe).
- Bij het verlaten van de werkplek worden schermen vergrendeld en actieve sessies afgesloten (clean screen-principe).
- Vertrouwelijke documenten worden afgedrukt, bewaard en vernietigd volgens de geldende richtlijnen inzake dataclassificatie en beveiligd afdrukken.
- De principes van clean desk en clean screen gelden eveneens bij telewerk en thuiswerk.

7.3 Delen van informatie

Het is verboden:

- patiëntinformatie te delen via privékanalen (zoals WhatsApp, privé e-mail, sociale media)
- gegevens door te geven zonder verificatie van identiteit en bevoegdheid
- vertrouwelijke of patiëntgerelateerde informatie op te slaan op niet-goedgekeurde gegevensdragers, persoonlijke toestellen of publieke cloudopslag.

Bij twijfel wordt steeds afgestemd met de leidinggevende.

7.4 Datalekken en incidenten

Mogelijke datalekken of inbreuken op informatieveiligheid worden onmiddellijk gemeld volgens de geldende procedure.

8. Gebruik van IT-middelen en communicatiesystemen

IT-middelen en communicatiesystemen worden op een veilige, zorgvuldige en professionele manier gebruikt.

- IT-systemen worden uitsluitend gebruikt voor professionele doeleinden
- Toegang tot systemen is persoonlijk en mag nooit gedeeld worden
- Medewerkers gaan zorgvuldig om met toegangen en wachtwoorden
- Toestellen worden vergrendeld bij afwezigheid
- Enkel beveiligde netwerken en toepassingen worden gebruikt

Alle activiteiten kunnen worden geregistreerd en gecontroleerd.

Het is verboden:

- niet-goedgekeurde software te installeren
- systemen te gebruiken voor illegale of ongepaste activiteiten
- vertrouwelijke informatie te verwerken via niet-beveiligde toepassingen

8.1 Informatiebeveiliging en cyberveilig gedrag

Medewerkers dragen actief bij aan de bescherming van informatie en systemen.

- Verdachte berichten (zoals phishing of sociale manipulatie) worden herkend en gemeld
- Beveiligingsincidenten en (mogelijke) datalekken worden onmiddellijk gemeld volgens de geldende procedure

Deze richtlijnen dragen bij aan het veilig en verantwoord gebruik van informatie en systemen, in lijn met de verplichtingen inzake informatiebeveiliging en de geldende regelgeving (zoals NIS2).

8.2 Gebruik van artificiële intelligentie (AI)

- **Gebruik** AI enkel ter ondersteuning van je werk en blijf altijd zelf verantwoordelijk voor inhoud, beslissingen en het eindresultaat.
- **Controleer** AI-output altijd kritisch op juistheid, volledigheid, context en actualiteit; corrigeer waar nodig en gebruik AI-output niet als enige bron.
- **Beperk** het gebruik van persoonlijke AI binnen het ziekenhuis tot de toegelaten AI-tools.
- **Pas** dataminimalisatie toe: deel enkel publieke of niet-gevoelige, geanonimiseerde informatie.
- **Deel of upload** nooit de volgende informatie in AI-tools:
 - patiëntgegevens en herleidbare informatie (o.a. namen, dossiernummers, geboortedata);

- (bijzondere) persoonsgegevens (o.a. medische, financiële/loongegevens);
- interne documenten, niet-gepubliceerde beleidsdocumenten en vertrouwelijke bedrijfsinformatie (o.a. strategie, audits, prognoses);
- juridisch vertrouwelijke informatie en gevoelige operationele/beveiligingsinformatie (o.a. toegangsstructuren, wachtwoordbeleid, kwetsbaarheden).
- **Vermeld** wanneer AI werd gebruikt bij het opstellen van documenten, adviezen of analyses.
- **Respecteer** auteursrechten en **verifieer** bronnen en referenties (AI kan foutieve of niet-bestaande verwijzingen genereren).
- **Neem** geen autonome zorgbeslissingen op basis van AI: laat AI niet autonoom leiden tot diagnose of behandeling zonder menselijke tussenkomst.
- **Meld** (mogelijke) datalekken, misbruik of incidenten onmiddellijk aan de DPO volgens de interne procedure.
- **Raadpleeg** de *gedragscode rond het gebruik van AI-tools* voor volledige regels, definities, toegelaten/verboden datatypes en licentieafspraken.

9. Social media en publieke communicatie

Medewerkers zijn ambassadeurs van het ziekenhuis.

Zij:

- delen hun mening op sociale media vanuit hun eigen naam en rol, en niet namens het ziekenhuis, tenzij ze daarvoor expliciet toestemming hebben
- delen geen vertrouwelijke of medische informatie
- respecteren privacy van patiënten en collega's
- communiceren respectvol en professioneel

Medewerkers reageren niet zelfstandig op negatieve berichtgeving, maar signaleren dit via de interne kanalen, d.w.z. via een Hartlink-chatbericht aan een van de collega's van de communicatiedienst of via communicatie@hhleuven.be.

10. Belangenconflicten en geschenken

Medewerkers handelen objectief en vermijden belangenconflicten.

- Persoonlijke belangen mogen professionele beslissingen niet beïnvloeden
- Mogelijke belangenconflicten worden gemeld

Het is verboden:

- geschenken of voordelen te aanvaarden zonder toestemming
- persoonlijk voordeel te halen uit de functie

11. Relaties met externe partners en leveranciers

Samenwerkingen gebeuren:

- objectief en transparant
- op basis van professionele criteria

Elke vorm van ongepaste beïnvloeding is niet toegestaan.

12. Veiligheid, welzijn en gezonde werkomgeving

Wij dragen samen verantwoordelijkheid voor een veilige werkomgeving.

- Veiligheidsvoorschriften worden nageleefd
- Incidenten en risico's worden gemeld
- Psychosociaal welzijn wordt actief bewaakt

Er is ondersteuning via:

- vertrouwenspersonen
- preventieadviseur
- externe preventiedienst

Agressie-incidenten worden opgevolgd en geanalyseerd.

13. Duurzaamheid en maatschappelijke verantwoordelijkheid

Als zorginstelling nemen wij onze verantwoordelijkheid op ten aanzien van mens, milieu en samenleving.

Wij:

- gaan bewust en zorgvuldig om met materialen, energie en middelen, met aandacht voor levenscyclus, hergebruik en verantwoorde afvalverwerking
- beperken verspilling en streven naar duurzame keuzes in ons dagelijkse handelen
- dragen bij aan een werkomgeving waarin respect, welzijn en lange termijn samenwerking centraal staan
- ondersteunen initiatieven die bijdragen aan een duurzame en toekomstgerichte zorgverlening

Duurzaamheid maakt integraal deel uit van professioneel en verantwoordelijk handelen binnen het ziekenhuis.

14. Meldingsprocedure bij inbreuken

Medewerkers worden aangemoedigd om inbreuken te melden via:

- leidinggevende
- HR
- vertrouwenspersonen
- preventieadviseur
- het integriteitsmeldingskanaal

Meldingen worden vertrouwelijk en zorgvuldig behandeld.

15. Bescherming van melders (klokkenluidersregeling)

Medewerkers die te goeder trouw een melding doen, worden beschermd tegen represailles.

Elke vorm van benadeling is verboden en kan aanleiding geven tot sancties.

16. Gevolgen van overtreding

Niet-naleving van deze gedragscode kan leiden tot maatregelen conform het arbeidsreglement, waaronder:

- schorsing
- schriftelijke vermaning
- beëindiging van de samenwerking (eventueel om dringende reden)

Indien nodig worden bevoegde instanties ingelicht.

Sancties worden op een consequente en proportionele manier toegepast.

17. Implementatie, communicatie en actualisatie

De gedragscode wordt:

- toegelicht bij indiensttreding
- beschikbaar gesteld via het intranet
- ondersteund via opleidingen en communicatie

Deze gedragscode maakt deel uit van het bredere kader van goed bestuur, integriteit en risicobeheer binnen het ziekenhuis en ondersteunt de naleving van relevante wet- en regelgeving (zoals onder meer NIS2 en GDPR).

De code wordt goedgekeurd door het Directiecomité en periodiek geëvalueerd en geactualiseerd.

18. Verklaring van kennisname en naleving

Elke medewerker verklaart:

- kennis te hebben genomen van deze gedragscode
- zich ertoe te verbinden deze na te leven

De gedragscode maakt integraal deel uit van het normatief kader van het ziekenhuis.

19. Referenties en onderliggende beleidsdocumenten

Deze gedragscode is gebaseerd op en dient gelezen te worden in samenhang met de geldende wetgeving (zoals onder meer NIS2 en GDPR) en interne beleidsdocumenten van het ziekenhuis.

De gedragscode sluit onder meer aan bij de volgende documenten (niet-limitatieve opsomming):

- het arbeidsreglement
- het IT- en informatiebeveiligingsbeleid
- het privacy- en gegevensbeschermingsbeleid (GDPR)
- de richtlijnen inzake het gebruik van artificiële intelligentie (AI gedragscode)
- het beleid rond psychosociaal welzijn en preventie
- procedures inzake integriteit, meldingskanalen en klokkenluidersregeling
- communicatiekompas
- procedure clean desk en clear screen beleid
- procedures in de kennisbank op Hartlink.

Bijlage 4: afspraken stage

Naam + voornaam van de stagiair(e): _____

Stageperiode: van _____ tot en met _____

Afdeling-stageplaats: _____

Door de stagiair bijlage 1,2, 3 en 4 gelezen, begrepen en

goedgekeurd Datum: _____

Naam+ voornaam: _____

Handtekening: _____